Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	98	("4333709" "4313952" "4245330" "5690946" "5661806" "5875404" "4342747" "6247837" "5511009" "4425624" "4559538" "6045761" "6165491" "6082672" "6222306" "6222306" "4307935" "4490808" "4477772" "4528498" "4505127" "5774357" "5500399" "4354262" "6216358" "6216358" "4865742" "6252059" "5422020" "6262409" "5867386" "5903454" "5920477" "5221453" "5483108" "4293412" "4439651" "4574301" "4774198" "6294180" PP11041 "5856088" "5068664" "5037822" "6356700" "4608092" "6344918" "4427658" "4860547").pn.	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/04/12 09:55
S1	17	"5987134"	US-PGPUB; USPAT; IBM_TDB	OR	OFF	2004/09/22 10:55
S2	1	"5987134".pn.	US-PGPUB; USPAT; IBM_TDB	OR	OFF	2004/09/22 14:58
S3	15	"5987134".URPN.	USPAT	OR	OFF	2004/09/22 10:57
S4	2	("4926480" | "5191611").PN.	USPAT	OR	OFF	2004/09/22 10:58
S5	1	"6651167".pn.	US-PGPUB; USPAT; IBM_TDB	OR	OFF	2004/09/22 14:58
S6	330	713/170.ccls.	US-PGPUB; USPAT; IBM_TDB	OR	OFF	2004/10/18 14:24
S7	1098	713/176.ccls.	US-PGPUB; USPAT; IBM_TDB	OR	OFF	2004/10/18 14:24
S8	51	713/174.ccls.	US-PGPUB; USPAT; IBM_TDB	OR	OFF	2004/10/18 15:01
S9	443	zero adj knowledge	US-PGPUB; USPAT; IBM_TDB	OR	OFF	2004/10/18 15:01
S10	249	zero adj knowledge and mod	US-PGPUB; USPAT; IBM_TDB	OR	OFF	2004/10/18 15:04
S11	198	zero adj knowledge and mod and authenti$5	US-PGPUB; USPAT; IBM_TDB	OR	OFF	2004/10/18 15:04

S12	170	zero adj knowledge and mod and authenti$5 and prime	US-PGPUB; USPAT; IBM_TDB	OR	OFF	2004/10/18 15:05
S13	151	zero adj knowledge and mod and authenti$5 and (prime$1 same public)	US-PGPUB; USPAT; IBM_TDB	OR	OFF	2004/10/18 15:09
S14	130	zero adj knowledge and mod and authenti$5 and (prime$1 same public) and private	US-PGPUB; USPAT; IBM_TDB	OR	OFF	2004/10/18 15:10
S15	9	zero adj knowledge and mod and authenti$5 and (prime$1 same public) and private and (chinese adj remainder$1)	US-PGPUB; USPAT; IBM_TDB	OR	OFF	2004/10/18 15:25
S16	3	guillou.in. and quisquater.in.	US-PGPUB; USPAT; IBM_TDB	OR	OFF	2004/10/18 15:25
S17	880	380/30.ccls.	US-PGPUB; USPAT; IBM_TDB	OR	OFF	2004/10/19 09:58
S18	653	380/30.ccls. and authentic$5	US-PGPUB; USPAT; IBM_TDB	OR	OFF	2004/10/19 09:58
S19	265	380/30.ccls. and authentic$5 and mod	US-PGPUB; USPAT; IBM_TDB	OR	OFF	2004/10/19 09:59
S20	240	380/30.ccls. and authentic$5 and mod and random	US-PGPUB; USPAT; IBM_TDB	OR	OFF	2004/10/19 09:59
S21	234	380/30.ccls. and authentic$5 and mod and signature$1	US-PGPUB; USPAT; IBM_TDB	OR	OFF	2004/10/19 09:59
S23	63194	"713"/("170" or "172" or "174" or "176" or "180").ccls.	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/03/22 13:41
S24	2090	(713/170 or 713/172 or 713/174 or 713/176 or 713/180).ccls.	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/03/22 13:42
S25	26	(713/170 or 713/172 or 713/174 or 713/176 or 713/180).ccls. and chinese adj remainder	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/03/22 13:42
S26	27	(713/170 or 713/172 or 713/174 or 713/176 or 713/180).ccls. and chinese adj remainder$1	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/03/22 14:04

S27	301	guillou.in. or quisqater.in.	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/03/22 14:05
S28	5	(guillou.in. or quisqater.in.) and (ring adj integers)	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/03/22 14:13
S29	61	(ring adj integers)	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/03/22 14:39
S30	0	(ring adj integers) and ".sup.2"	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/03/22 14:12
S31	0	".sup.2"	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/03/22 14:12
S32	0	"$.sup.2"	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/03/22 14:12
S33	97	"a.sup.p"	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/03/22 14:13
S34	11170	"a.sup.2"	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/03/22 14:13
S35	0	"$.sup.2"	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/03/22 14:13
S36	18665	"x.sup.2"	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/03/22 14:13
S37	0	"x.sup.2" with (ring adj integers)	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/03/22 14:14
S38	0	"x.sup.2" same (ring adj integers)	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/03/22 14:14

S39	207	"x.sup.2" same (mod)	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/03/22 14:14
S40	192	"x.sup.2" with (mod)	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/03/22 14:14
S41	0	"x.sup.2" with (mod) with "g.sub. i"	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/03/22 14:15
S42	2	"x.sup.2" with (mod) and ring adj integers	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/03/22 14:25
S43	5	non$1quadratic adj residue	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/03/22 14:25
S44	9	non$1quadratic adj residue$1	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/03/22 14:25
S45	721	telediffusion.as.	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/03/22 14:39
S46	9	telediffusion.as. and authenticat$3	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/03/22 14:45
S47	21	kawamura.in. and shimbo.in.	US-PGPUB; USPAT; DERWENT; IBM_TDB	OR	OFF	2005/03/22 14:45

Your search matched **30** of **1140634** documents.
A maximum of **500** results are displayed, **15** to a page, sorted by **Relevance Descending** order.

Refine This Search:
You may refine your search by editing the current search expression or enterin new one in the text box.

guillou <or> quisquater Search

☐ Check to search within this result set

Results Key:
JNL = Journal or Magazine **CNF** = Conference **STD** = Standard

---

1 **Cryptology for digital TV broadcasting**
Macq, B.M.; Quisquater, J.-J.;
Proceedings of the IEEE , Volume: 83 , Issue: 6 , June 1995
Pages:944 - 957

[Abstract] [PDF Full-Text (1356 KB)] **IEEE JNL**

---

2 **Electronic Systems and Equipment for Evolving Loop Plant**
Le Guillou, J.-A.; Pernin, J.-L.; Schwartz, A.;
Communications, IEEE Transactions on [legacy, pre - 1988] , Volume: 28 , Iss 7 , Jul 1980
Pages:967 - 975

[Abstract] [PDF Full-Text (944 KB)] **IEEE JNL**

---

3 **PRANA at the Age of Four: Multiservice Loops Reach Out**
Le Guillou, J.-A.; Marcel, F.; Schwartz, A.;
Communications, IEEE Transactions on [legacy, pre - 1988] , Volume: 30 , Iss 9 , Sep 1982
Pages:2185 - 2210

[Abstract] [PDF Full-Text (2640 KB)] **IEEE JNL**

---

4 **SCALPS: Smart card for limited payment systems**
Dhem, J.-F.; Veithen, D.; Quisquater, J.-J.;
Micro, IEEE , Volume: 16 , Issue: 3 , June 1996
Pages:42 - 51

[Abstract] [PDF Full-Text (1968 KB)] **IEEE JNL**

---

5 **Chinese lotto as an exhaustive code-breaking machine**
Quisquater, J.-J.; Desmedt, Y.G.;
Computer , Volume: 24 , Issue: 11 , Nov. 1991
Pages:14 - 22

[Abstract] [PDF Full-Text (856 KB)] **IEEE JNL**

---

6 **Hardware security for software privacy support**
Gilmont, T.; Legat, J.-D.; Quisquater, J.-J.;
Electronics Letters , Volume: 35 , Issue: 24 , 25 Nov. 1999
Pages:2096 - 2098

[Abstract] [PDF Full-Text (244 KB)] IEE JNL

---

7 **Cryptosystem of Chua and Ling**
Joye, M.; Quisquater, J.-J.;
Electronics Letters , Volume: 33 , Issue: 23 , 6 Nov. 1997
Pages:1938

[Abstract] [PDF Full-Text (116 KB)] IEE JNL

---

8 **Normalisation in diminished-radix modulus transformation**
Dhem, J.-F.; Joye, M.; Quisquater, J.-J.;
Electronics Letters , Volume: 33 , Issue: 23 , 6 Nov. 1997
Pages:1931

[Abstract] [PDF Full-Text (108 KB)] IEE JNL

---

9 **Efficient computation of full Lucas sequences**
Joye, M.; Quisquater, J.-J.;
Electronics Letters , Volume: 32 , Issue: 6 , 14 March 1996
Pages:537 - 538

[Abstract] [PDF Full-Text (204 KB)] IEE JNL

---

10 **Luminescence of erbium implanted in various semiconductors: IV, I and II-VI materials**
Favennec, P.N.; L'Haridon, H.; Salvi, M.; Moutonnet, D.; Le Guillou, Y.;
Electronics Letters , Volume: 25 , Issue: 11 , 25 May 1989
Pages:718 - 719

[Abstract] [PDF Full-Text (196 KB)] IEE JNL

---

11 **Handling dynamic changes in hierarchical radiosity through interac meshes**
Carre, S.; Deniel, J.M.; Guillou, E.; Bouatouch, K.;
Computer Graphics and Applications, 2000. Proceedings. The Eighth Pacific Conference on , 3-5 Oct. 2000
Pages:40 - 436

[Abstract] [PDF Full-Text (1148 KB)] IEEE CNF

---

12 **Context-oriented coding aids for healthcare activity description**
Cauvin, J.M.; Mansourati, J.; Scheydeker, J.L.; Le Guillou, C.; Solaiman, B.; B J.J.;
Information Technology Applications in Biomedicine, 2000. Proceedings. 2000 EMBS International Conference on , 9-10 Nov. 2000
Pages:89 - 94

[Abstract] [PDF Full-Text (448 KB)] IEEE CNF

---

13 **Information processing in upper digestive endoscopy**
Le Guillou, C.; Cauvin, J.-M.; Solaiman, B.; Robaszkiewicz, M.; Roux, C.;
Information Technology Applications in Biomedicine, 2000. Proceedings. 2000 EMBS International Conference on , 9-10 Nov. 2000
Pages:183 - 188

[Abstract] [PDF Full-Text (716 KB)] **IEEE CNF**

14 **Smart card circuits in SOI technology**
Neve, A.; Flandre, D.; Quisquater, J.-J.;
SOI Conference, 2000 IEEE International , 2-5 Oct. 2000
Pages:48 - 49

[Abstract] [PDF Full-Text (100 KB)] **IEEE CNF**

15 **Knowledge representation and cases indexing in upper digestive endoscopy**
Le Guillou, C.; Cauvin, J.-M.; Solaiman, B.; Robaszkiewicz, M.; Roux, C.;
Engineering in Medicine and Biology Society, 2000. Proceedings of the 22nd A International Conference of the IEEE , Volume: 1 , 23-28 July 2000
Pages:9 - 12 vol.1

[Abstract] [PDF Full-Text (596 KB)] **IEEE CNF**

1 2 Next

Your search matched **30** of **1140634** documents.
A maximum of **500** results are displayed, **15** to a page, sorted by **Relevance Descending** order.

Refine This Search:
You may refine your search by editing the current search expression or enterin new one in the text box.

guillou <or> quisquater Search

☐ Check to search within this result set

Results Key:
JNL = Journal or Magazine **CNF** = Conference **STD** = Standard

---

16 **Diagnostic reasoning by classification in upper digestive tract endoscopy**
Cauvin, J.-M.; Le Guillou, C.; Solaiman, B.; Robaszkiewicz, M.; Gouerou, H.; R C.;
Engineering in Medicine and Biology Society, 2000. Proceedings of the 22nd A International Conference of the IEEE , Volume: 1 , 23-28 July 2000
Pages:31 - 34 vol.1

[Abstract] [PDF Full-Text (272 KB)] **IEEE CNF**

---

17 **Automatic design of VLSI pipelined LMS architectures**
Guillou, A.-C.; Quinton, P.; Risset, T.; Massicotte, D.;
Parallel Computing in Electrical Engineering, 2000. PARELEC 2000. Proceeding International Conference on , 27-30 Aug. 2000
Pages:144 - 149

[Abstract] [PDF Full-Text (416 KB)] **IEEE CNF**

---

18 **Fabrication and performance of mesa interconnect**
Carley, L.R.; Guillou, D.F.; Santhanam, S.;
Low Power Electronics and Design, 1996., International Symposium on , 12-14 Aug. 1996
Pages:133 - 137

[Abstract] [PDF Full-Text (568 KB)] **IEEE CNF**

---

19 **Laminated high-aspect-ratio microstructures in a conventional CMO process**
Fedder, G.K.; Santhanam, S.; Reed, M.L.; Eagle, S.C.; Guillou, D.F.; Lu, M.S.- Carley, L.R.;
Micro Electro Mechanical Systems, 1996, MEMS '96, Proceedings. 'An Investiga of Micro Structures, Sensors, Actuators, Machines and Systems'. IEEE, The Nin Annual International Workshop on , 11-15 Feb. 1996
Pages:13 - 18

[Abstract] [PDF Full-Text (1188 KB)] **IEEE CNF**

---

20 **Enhancing security in the memory management unit**
Gilmont, T.; Legat, J.-D.; Quisquater, J.-J.;
EUROMICRO Conference, 1999. Proceedings. 25th , Volume: 1 , 8-10 Sept. 19
Pages:449 - 456 vol.1

[Abstract] [PDF Full-Text (92 KB)] **IEEE CNF**

---

21 **Deriving a role-based access control model from the OBBAC model**
Kabasele Tenday, J.M.; Quisquater, J.-J.; Lobelle, M.;
Enabling Technologies: Infrastructure for Collaborative Enterprises, 1999. (WE ICE '99) Proceedings. IEEE 8th International Workshops on , 16-18 June 1999
Pages:147 - 151

[Abstract] [PDF Full-Text (56 KB)] **IEEE CNF**

---

22 **Diagnostic reasoning in digestive tract endoscopy**
Cauvin, J.-M.; Le Guillou, C.; Solaiman, B.; Robaszkiewicz, M.; Gouerou, H.; R C.;
[Engineering in Medicine and Biology, 1999. 21st Annual Conf. and the 1999 Annual Fall Meeting of the Biomedical Engineering Soc.] BMES/EMBS Conferen 1999. Proceedings of the First Joint , Volume: 2 , 13-16 Oct. 1999
Pages:1241 vol.2

[Abstract] [PDF Full-Text (64 KB)] **IEEE CNF**

---

23 **"Multi-agent" approach in endoscopic images diagnosis aid**
Le Guillou, C.; Cauvin, J.-M.; Solaiman, B.; Robaszkiewicz, M.; Roux, C.;
[Engineering in Medicine and Biology, 1999. 21st Annual Conf. and the 1999 Annual Fall Meeting of the Biomedical Engineering Soc.] BMES/EMBS Conferen 1999. Proceedings of the First Joint , Volume: 2 , 13-16 Oct. 1999
Pages:1237 vol.2

[Abstract] [PDF Full-Text (84 KB)] **IEEE CNF**

---

24 **Timestamps: main issues on their use and implementation**
Massias, H.; Serret Avila, X.; Quisquater, J.-J.;
Enabling Technologies: Infrastructure for Collaborative Enterprises, 1999. (WE ICE '99) Proceedings. IEEE 8th International Workshops on , 16-18 June 1999
Pages:178 - 183

[Abstract] [PDF Full-Text (84 KB)] **IEEE CNF**

---

25 **Case-based reasoning (CBR) in endoscopic images diagnosis aid**
Le Guillou, C.; Cauvin, J.-M.; Solaiman, B.; Robaszkiewicz, M.; Roux, C.;
[Engineering in Medicine and Biology, 1999. 21st Annual Conf. and the 1999 Annual Fall Meeting of the Biomedical Engineering Soc.] BMES/EMBS Conferen 1999. Proceedings of the First Joint , Volume: 2 , 13-16 Oct. 1999
Pages:1236 vol.2

[Abstract] [PDF Full-Text (80 KB)] **IEEE CNF**

---

26 **Reference database of images and video sequences in gastrointesti endoscopy: a medical approach**
Cauvin, J.M.; Solaiman, B.; Le Guillou, C.; Brunet, G.; Robaszkiewicz, M.; Rou C.;
Engineering in Medicine and Biology Society, 1998. Proceedings of the 20th An International Conference of the IEEE , Volume: 2 , 29 Oct.-1 Nov. 1998
Pages:978 - 981 vol.2

[Abstract] [PDF Full-Text (748 KB)] **IEEE CNF**

27 **Observations of water vapour absorption using airborne microwave radiometers at 89 and 157 GHz**
English, S.J.; Jones, D.C.; Rayer, P.J.; Hewison, T.J.; Saunders, R.W.; Guillou Prigent, C.; Wang, J.; Anderson, G.;
Geoscience and Remote Sensing Symposium, 1995. IGARSS '95. 'Quantitative Remote Sensing for Science and Applications', International , Volume: 2 , 10-1 July 1995
Pages:1395 - 1397 vol.2

[Abstract] [PDF Full-Text (292 KB)] **IEEE CNF**

---

28 **Sea surface emissivity models at millimeter waves: validation from aircraft measurements at 89 and 157 GHz**
Guillou, C.; Prigent, C.; English, S.; Jones, D.;
Geoscience and Remote Sensing Symposium, 1993. IGARSS '93. 'Better Understanding of Earth Environment'., International , 18-21 Aug. 1993
Pages:1619 - 1621 vol.4

[Abstract] [PDF Full-Text (176 KB)] **IEEE CNF**

---

29 **ID-based group signature**
Sangjoon Park; Seungjoo Kim; Dongho Won;
Electronics Letters , Volume: 33 , Issue: 19 , 11 Sept. 1997
Pages:1616 - 1617

[Abstract] [PDF Full-Text (276 KB)] **IEE JNL**

---

30 **Bulk encryption algorithm for use with RSA**
Sewell, R.F.;
Electronics Letters , Volume: 29 , Issue: 25 , 9 Dec. 1993
Pages:2183 - 2185

[Abstract] [PDF Full-Text (292 KB)] **IEE JNL**

IEEE Xplore® RELEASE 1.8

Welcome
United States Patent and Trademark Office

Your search matched **0** of **1140634** documents.
A maximum of **500** results are displayed, **15** to a page, sorted by **Relevance Descending** order.

Refine This Search:
You may refine your search by editing the current search expression or enterin new one in the text box.

gq2 Search

☐ Check to search within this result set

Results Key:
JNL = Journal or Magazine **CNF** = Conference **STD** = Standard

---

Results:
No documents matched your query.

Your search matched **0** of **1140634** documents.
A maximum of **500** results are displayed, **15** to a page, sorted by **Relevance Descending** order.

Refine This Search:
You may refine your search by editing the current search expression or enterin new one in the text box.

ring <and> integers <and> authenticate Search

☐ Check to search within this result set

Results Key:
JNL = Journal or Magazine **CNF** = Conference **STD** = Standard

---

Results:
No documents matched your query.

Terms used **guillou quisquater**

Found **9** of **151,219**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

☐ Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 9 of 9

Relevance scale

1 Fabrication and performance of mesa interconnect

L. Carley, D. Guillou, S. Santhanam

August 1996 **Proceedings of the 1996 international symposium on Low power electronics and design**

Full text available: pdf(80.29 KB) Additional Information: full citation, references, index terms

2 Reconfigurable hardware solutions for the digital rights management of digital cinema

G. Rouvroy, F.-X. Standaert, F. Lefèbvre, J.-J. Quisquater, B. Macq, J.-D. Legat

October 2004 **Proceedings of the 4th ACM workshop on Digital rights management**

Full text available: pdf(440.86 KB) Additional Information: full citation, abstract, references, index terms

This paper presents a hardware implementation of a decoder for Digital Cinema images. This decoder enables us to deal with image size of 2K with 24 frames per second and 36 bits per pixels. It is the first implementation known nowadays that perfectly fits in one single Virtex-II® FPGA and includes AES decryption, JPEG 2000 decompression and fingerprinting blocks. This hardware offers therefore high-quality image processing as well as robust security.

Keywords: AES, DRM, FPGA, JPEG 2000, digital cinema, watermarking

3 Efficient revocation and threshold pairing based cryptosystems

Benoît Libert, Jean-Jacques Quisquater

July 2003 **Proceedings of the twenty-second annual symposium on Principles of distributed computing**

Full text available: pdf(1.02 MB) Additional Information: full citation, abstract, references, index terms

Boneh, Ding, Tsudik and Wong recently proposed a way for obtaining fast revocation of RSA keys. Their method consists in using security mediators that keep a piece of each user's private key in such a way that every decrytion or signature operation requires the help of the mediator for the user. Revocation is achieved by instructing the mediator to stop helping the user to sign or decrypt messages. This security architecture, called SEM, gave rise to an identity based mediated RSA scheme (IB-mRS ...

Keywords: Public key cryptosystems, bilinear maps, revocation

4 Poster session: Design strategies and modified descriptions to optimize cipher FPGA implementations: fast and compact results for DES and triple-DES

Gaël Rouvroy, Francois-Xavier Standaert, Jean-Jacques Quisquater, Jean-Didier Legat

February 2003 **Proceedings of the 2003 ACM/SIGDA eleventh international symposium**

on Field programmable gate arrays

Full text available: pdf(187.05 KB) Additional Information: full citation, abstract

We propose a new mathematical DES description that allows optimized implementations. It also provides the best DES and triple-DES FPGA implementations known in term of ratio throughput/area, where area means the number of FPGA slices used. First, we get a less resource consuming unrolled DES implementation that works at data rates of 21.3 Gbps (333 MHz), using VIRTEX II technology. In this design, the plaintext, the key and the mode (encryption/decrytion) can be changed on a cycle-by-cycle basis ...

5 Applications: A methodology to implement block ciphers in reconfigurable hardware and its application to fast and compact AES RIJNDAEL

François-Xavier Standaert, Gael Rouvroy, Jean-Jacques Quisquater, Jean-Didier Legat

February 2003 **Proceedings of the 2003 ACM/SIGDA eleventh international symposium on Field programmable gate arrays**

Full text available: pdf(236.87 KB) Additional Information: full citation, abstract, references, index terms

Reprogrammable devices such as Field Programmable Gate Arrays (FPGA's) are highly attractive options for hardware implementations of encryption algorithms and this report investigates a methodology to efficiently implement block ciphers in CLB-based FPGA's. Our methodology is applied to the new Advanced Encryption Standard RIJNDAEL and the resulting designs offer better performances than previously published in literature. We propose designs that unroll the 10 AES rounds and pipeline them in ord ...

Keywords: AES RIJNDAEL, FPGA, cryptography, high encryption rates, reconfigurable hardware

6 Security protocols: Security analysis of the cliques protocols suites: first results

O. Pereira, J-J. Quisquater

June 2001 **Proceedings of the 16th international conference on Information security: Trusted information: the new decade challenge**

Additional Information: full citation, abstract, references, index terms

The Cliques protocols are extensions of the Diffie-Hellman key exchange protocol to a group settings. In this paper, we are analyzing the A -GDH.2 suite that is intended to allow a group to share an authenticated key and to perform dynamic changes in the group constitution (adding and deleting member). We are proposing an original method to analyze these protocols and are presenting a number of unpublished flaws with respect to each of the main security properties claimed in protocol definitions ...

Keywords: Diffie-Hellman, cliques protocols, group protocols, systematic analysis

7 Group Key Management and Signatures: Provably authenticated group Diffie-Hellman key exchange

Emmanuel Bresson, Olivier Chevassut, David Pointcheval, Jean-Jacques Quisquater

November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security**

Full text available: pdf(578.14 KB) Additional Information: full citation, abstract, references, citings, index terms

Group Diffie-Hellman protocols for Authenticated Key Exchange (AKE) are designed to provide a pool of players with a shared secret key which may later be used, for example, to achieve multicast message integrity. Over the years, several schemes have been offered. However, no formal treatment for this cryptographic problem has ever been suggested. In this paper, we present a security model for this problem and use it to precisely define AKE (with "implicit" authentication) as the fundamental goal ...

8 On the importance of securing your bins: the garbage-man-in-the-middle attack

Marc Joye, Jean-Jacques Quisquater

April 1997 **Proceedings of the 4th ACM conference on Computer and communications security**

Full text available: pdf(812.52 KB) Additional Information: full citation, references, index terms

9 Securing Mobile Appliances: New Challenges for the System Designer

Anand Raghunathan, Srivaths Ravi, Sunil Hattangady, Jean-Jacques Quisquater

March 2003 **Proceedings of the conference on Design, Automation and Test in Europe - Volume 1**

Full text available: Publisher Site Additional Information: full citation, abstract

As intelligent electronic systems pervade all aspects of our lives, capturing, storing, and communicating a wide range of sensitive and personal data, security is emerging as a critical concern that must be addressed in order to enable several current and future applications. Mobile appliances, which will play a critical role in enabling the visions of ubiquitous computing and communications, and ambient intelligence, are perhaps the most challenging to secure ¿ they often rely on a public mediu ...

Results 1 - 9 of 9

Terms used **guillou quisquater**

Found **128** of **151,219**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

☐ Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 128

Result page: **1** 2 3 4 5 6 7 next

Relevance scale

1 Verifiable encryption of digital signatures and applications

Giuseppe Ateniese

February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 1

Full text available: pdf(258.12 KB) Additional Information: full citation, abstract, references, index terms

This paper presents a new simple schemes for verifiable encryption of digital signatures. We make use of a trusted third party (TTP) but in an *optimistic* sense, that is, the TTP takes part in the protocol only if one user cheats or simply crashes. Our schemes can be used as primitives to build efficient fair exchange and certified e-mail protocols.

Keywords: Certified e-mail, contract signing, digital signatures, fair exchange, proof of knowledge, public-key cryptography

2 New blind signatures equivalent to factorization (extended abstract)

David Pointcheval, Jacques Stern

April 1997 **Proceedings of the 4th ACM conference on Computer and communications security**

Full text available: pdf(776.77 KB) Additional Information: full citation, references, citings, index terms

3 Practical multi-candidate election system

Olivier Baudron, Pierre-Alain Fouque, David Pointcheval, Jacques Stern, Guillaume Poupard

August 2001 **Proceedings of the twentieth annual ACM symposium on Principles of distributed computing**

Full text available: pdf(898.50 KB) Additional Information: full citation, abstract, references, index terms

The aim of electronic voting schemes is to provide a set of protocols that allow voters to cast ballots while a group of authorities collect the votes and output the final tally. In this paper we describe a practical multi-candidate election scheme that guarantees privacy of voters, public verifiability, and robustness against a coalition of malicious authorities. Furthermore, we address the problem of receipt-freeness and incoercibility of voters. Our new scheme is based on the Paillier cryp ...

4 Efficient verifiable encryption (and fair exchange) of digital signatures

Giuseppe Ateniese

November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**

Full text available: pdf(781.40 KB) Additional Information: full citation, abstract, references, citings, index terms

A fair exchange protocol allows two users to exchange items so that either each user gets the other's item or neither user does. In [2], verifiable encryption is introduced as a

primitive that can be used to build extremely efficient fair exchange protocols where the items exchanged represent digital signatures. Such protocols may be used to digitally sign contracts.This paper presents new simple schemes for verifiable encryption of digital signatures. We make us ...

Keywords: contract signing problem, digital signatures, fair exchange, proof of knowledge, public-key cryptography, verifiable encryption

5 Anonymous authentication with subset queries (extended abstract)

Dan Boneh, Matt Franklin

November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**

Full text available: pdf(613.93 KB) Additional Information: full citation, abstract, references, citings, index terms

We develop new schemes for anonymous authentication that support identity escrow. Our protocols also allow a prover to demonstrate membership in an arbitrary subset of users; key revocation is an important special case of this feature. Using the Fiat-Shamir heuristic, our interactive authentication protocols yield new constructions for non-interactive group signature schemes. We use the higher-residuosity assumption, which leads to greater efficiency and more natural security proofs than pr ...

Keywords: anonymous authentication, group signature, identity escrow

6 On the fly signatures based on factoring

Guillaume Poupard, Jacques Stern

November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**

Full text available: pdf(786.71 KB) Additional Information: full citation, abstract, references, index terms

In response to the current need for fast, secure and cheap public-key cryptography largely induced by the fast development of electronic commerce, we propose a new on the fly signature scheme, i.e. a scheme that requires very small on-line work for the signer It combines provable security based on the factorization problem, short public and secret keys, short transmission and minimal on-line computation. It is the first RSA-like signature scheme that can be used for both ef ...

7 Signature schemes based on the strong RSA assumption

Ronald Cramer, Victor Shoup

August 2000 **ACM Transactions on Information and System Security (TISSEC)**, Volume 3 Issue 3

Full text available: pdf(168.52 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We describe and analyze a new digital signature scheme. The new scheme is quite efficient, does not require the signer to maintain any state, and can be proven secure against adaptive chosen message attack under a reasonable intractability assumption, the so-called strong RSA assumption. Moreover, a hash function can be incorporated into the scheme in such a way that it is also secure in the random oracle model under the standard RSA assumption.

Keywords: RSA, digital signatures, provable security

8 Efficient revocation and threshold pairing based cryptosystems

Benoît Libert, Jean-Jacques Quisquater

July 2003 **Proceedings of the twenty-second annual symposium on Principles of distributed computing**

Full text available: pdf(1.02 MB) Additional Information: full citation, abstract, references, index terms

Boneh, Ding, Tsudik and Wong recently proposed a way for obtaining fast revocation of RSA keys. Their method consists in using security mediators that keep a piece of each user's

private key in such a way that every decrytion or signature operation requires the help of the mediator for the user. Revocation is achieved by instructing the mediator to stop helping the user to sign or decrypt messages. This security architecture, called SEM, gave rise to an identity based mediated RSA scheme (IB-mRS ...

Keywords: Public key cryptosystems, bilinear maps, revocation

9 Authentication and signature schemes: On the performance, feasibility, and use of forward-secure signatures

Eric Cronin, Sugih Jamin, Tal Malkin, Patrick McDaniel

October 2003 **Proceedings of the 10th ACM conference on Computer and communications security**

Full text available: pdf(386.51 KB) Additional Information: full citation, abstract, references, index terms

Forward-secure signatures (FSSs) have recently received much attention from the cryptographic theory community as a potentially realistic way to mitigate many of the difficulties digital signatures face with key exposure. However, no previous works have explored the practical performance of these proposed constructions in real-world applications, nor have they compared FSS to traditional, non-forward-secure, signatures in a non-asymptotic way.We present an empirical evaluation of several FSS sch ...

Keywords: digital signatures, forward-secure signatures

10 Fine-grained control of security capabilities

Dan Boneh, Xuhua Ding, Gene Tsudik

February 2004 **ACM Transactions on Internet Technology (TOIT)**, Volume 4 Issue 1

Full text available: pdf(128.09 KB) Additional Information: full citation, abstract, references, index terms

We present a new approach for fine-grained control over users' security privileges (fast revocation of credentials) centered around the concept of an on-line semi-trusted mediator (SEM). The use of a SEM in conjunction with a simple threshold variant of the RSA cryptosystem (mediated RSA) offers a number of practical advantages over current revocation techniques. The benefits include simplified validation of digital signatures, efficient certificate revocation for legacy systems and fast revocat ...

Keywords: Certificate Revocation, Digital Signatures, Public Key Infrastructure

11 Efficient generation of shared RSA keys

Dan Boneh, Matthew Franklin

July 2001 **Journal of the ACM (JACM)**, Volume 48 Issue 4

Full text available: pdf(202.94 KB) Additional Information: full citation, abstract, references, citings, index terms

We describe efficient techniques for a number of parties to jointly generate an RSA key. At the end of the protocol an RSA modulus $N = pq$ is publicly known. None of the parties know the factorization of N. In addition a public encryption exponent is publicly known and each party holds a share of the private exponent that enables threshold decryption. Our protocols are efficient in computation and communication. All results are presented in the *honest but curious* scena ...

Keywords: Multiparty computation, RSA, primality testing, threshold cryptography

12 The random oracle methodology, revisited

Ran Canetti, Oded Goldreich, Shai Halevi

July 2004 **Journal of the ACM (JACM)**, Volume 51 Issue 4

Full text available: pdf(334.81 KB) Additional Information: full citation, abstract, references, index terms

We take a critical look at the relationship between the security of cryptographic schemes in the Random Oracle Model, and the security of the schemes that result from implementing

the random oracle by so called "cryptographic hash functions".The main result of this article is a negative one: There exist signature and encryption schemes that are secure in the Random Oracle Model, but for which *any implementation* of the random oracle results in insecure schemes. In the process of devising t ...

Keywords: CS-proofs, Correlation intractability, cryptography, diagonalization, the random-oracle model

13 Session 8A: Non-interactive and reusable non-malleable commitment schemes 
Ivan Damgard, Jens Groth
June 2003 **Proceedings of the thirty-fifth annual ACM symposium on Theory of computing**
Full text available: pdf(333.10 KB) Additional Information: full citation, abstract, references, index terms

We consider non-malleable (NM) and universally composable (UC) commitment schemes in the common reference string (CRS) model. We show how to construct non-interactive NM commitments that remain non-malleable even if the adversary has access to an arbitrary number of commitments from honest players - rather than one, as in several previous schemes. We show this is a strictly stronger security notion. Our construction is the first non-interactive scheme achieving this that can be based on the mini ...

Keywords: commitment, non-malleability, one-way function, signature, universal composability

14 Agents, interactions, mobility and systems: Blinded-key signatures: securing private keys embedded in mobile agents 
Lucas C. Ferreira, Ricardo Dahab
March 2002 **Proceedings of the 2002 ACM symposium on Applied computing**
Full text available: pdf(442.06 KB) Additional Information: full citation, abstract, references, index terms

We present a new cryptographic primitive, the *blinded-key signature,* which allows the inclusion of private keys in autonomous mobile agents. This novel approach can be applied to many well-known digital signature schemes, such as RSA and ElGammal.

Keywords: cryptography, digital signatures, mobile agents, security

15 Signature schemes based on the strong RSA assumption 
Ronald Cramer, Victor Shoup
November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**
Full text available: pdf(530.95 KB) Additional Information: full citation, abstract, references, citings, index terms

We describe and analyze a new digital signature scheme. The new scheme is quite efficient, does not require the the signer to maintain any state, and can be proven secure against adaptive chosen message attack under a reasonable intractability assumption, the so-called strong RSA assumption. Moreover, a hash function can be incorporated into the scheme in such a way that it is also secure in the random oracle model under the standard RSA assumption.

16 An optimally robust hybrid mix network 
Markus Jakobsson, Ari Juels
August 2001 **Proceedings of the twentieth annual ACM symposium on Principles of distributed computing**
Full text available: pdf(858.02 KB) Additional Information: full citation, abstract, references, citings, index terms

We present a mix network that achieves efficient integration of public-key and symmetric-key operations. This *hybrid* mix network is capable of natural processing of arbitrarily long input elements, and is fast in both practical and asymptotic senses. While the overhead in

the size of input elements is linear in the number of mix servers, it is quite small in practice. In contrast to previous hybrid constructions, ours has optimal robustness, that is, robustness against any minority coa ...

17 The Ω key management service
Michael K. Reiter, Matthew K. Franklin, John B. Lacy, Rebecca N. Wright
January 1996 **Proceedings of the 3rd ACM conference on Computer and communications security**
Full text available: pdf(1.37 MB) Additional Information: full citation, references, citings, index terms

18 Distributing trust with the Rampart toolkit
Michael Reiter
April 1996 **Communications of the ACM**, Volume 39 Issue 4
Full text available: pdf(170.20 KB) Additional Information: full citation, references, citings, index terms, review

19 Session 1: Applications: New directions for integrated circuit cards operating systems
Pierre Paradinas, Jean-Jacques Vandewalle
September 1994 **Proceedings of the 6th workshop on ACM SIGOPS European workshop: Matching operating systems to application needs**
Full text available: pdf(437.96 KB) Additional Information: full citation, abstract, references

Integrated circuit cards or smart cards are now well-known. Applications such as electronic purses (cash units stored in cards), subscriber identification cards used in cellular telephone or access keys for pay-TV and information highways emerge in many places with millions of users. More services are required by applications providers and card holders. Mainly, new integrated circuit cards evolve towards non-predefined multi-purpose, open and multi-user applications. Today, operating systems imp ...

Keywords: Integrated Circuit Card Applications, Integrated Circuit Card Operating System, Object-Oriented Technologies, Secured method execution

20 Funkspiel schemes: an alternative to conventional tamper resistance
Johan Håstad, Jakob Jonsson, Ari Juels, Moti Yung
November 2000 **Proceedings of the 7th ACM conference on Computer and communications security**
Full text available: pdf(528.32 KB) Additional Information: full citation, references, citings, index terms

Term used **gq2**

Found **13** of **151,219**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

☐ Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 13 of 13

Relevance scale

1 The first-order theory of subtyping constraints

Zhendong Su, Alexander Aiken, Joachim Niehren, Tim Priesnitz, Ralf Treinen

January 2002 **ACM SIGPLAN Notices , Proceedings of the 29th ACM SIGPLAN-SIGACT symposium on Principles of programming languages**, Volume 37 Issue 1

Full text available: pdf(489.49 KB) Additional Information: full citation, abstract, references, citings

We investigate the first-order of subtyping constraints. We show that the first-order theory of non-structural subtyping is undecidable, and we show that in the case where all constructors are either unary or nullary, the first-order theory is decidable for both structural and non-structural subtyping. The decidability results are shown by reduction to a decision problem on tree automata. This work is a step towards resolving long-standing open problems of the decidability of entailment for non- ...

2 The BEA streaming XQuery processor

Daniela Florescu, Chris Hillery, Donald Kossmann, Paul Lucas, Fabio Riccardi, Till Westmann, J. Carey, Arvind Sundararajan

September 2004 **The VLDB Journal — The International Journal on Very Large Data Bases**, Volume 13 Issue 3

Full text available: pdf(328.94 KB) Additional Information: full citation, abstract

This paper describes the design, implementation, and performance characteristics of a commercial XQuery processing engine, the BEA streaming XQuery processor. This XQuery engine was designed to provide high performance for message-processing applications, i.e., for transforming XML data streams. The engine is a central component of the 8.1 release of BEA's WebLogic Integration (WLI) product. The BEA XQuery engine is fully compliant with the August 2002 draft of the W3C XML Query Langua ...

3 Effects of spatial audio on memory, comprehension, and preference during desktop conferences

Jessica J. Baldis

March 2001 **Proceedings of the SIGCHI conference on Human factors in computing systems**

Full text available: pdf(288.08 KB) Additional Information: full citation, abstract, references, citings, index terms

An experiment was conducted to determine the effect of spatial audio on memory, focal assurance, perceived comprehension and listener preferences during desktop conferences. Nineteen participants listened to six, pre-recorded, desktop conferences. Each conference was presented using either non-spatial audio, co-located spatial audio, or scaled spatial audio, and during half of the conferences, static visual representations of the conferees were present. In the co-located condition, each con ...

Keywords: 3D, audio, communication, comprehension, focal assurance, memory, perception, sound, spatial, user preference

4 A new effective and efficient multi-level partitioning algorithm
Youssef Saab
January 2000 **Proceedings of the conference on Design, automation and test in Europe**

Full text available: pdf(174.97 KB) Publisher Site

Additional Information: full citation, references

5 Deciding branching time logic
E. Allen Emerson, A. Prasad Sistla
December 1984 **Proceedings of the sixteenth annual ACM symposium on Theory of computing**

Full text available: pdf(930.00 KB)

Additional Information: full citation, abstract, references, citings, index terms

In this paper we study the full branching time logic (CTL*) in which a path quantifier, either A ("for all paths-&-rdquo;) or E (-&-ldquo;for some path"), prefixes an assertion composed of arbitrary combinations of the usual linear time operators F ("sometime"), G ("always"), X ("nexttime"), and U ("until"). We show that the problem of determining if a CTL* formula is satisfiable in structure generated by a binary relation is decid ...

6 "Sometimes" and "not never" revisited: on branching versus linear time temporal logic
E. Allen Emerson, Joseph Y. Halpern
January 1986 **Journal of the ACM (JACM)**, Volume 33 Issue 1

Full text available: pdf(2.07 MB)

Additional Information: full citation, abstract, references, citings, index terms, review

The differences between and appropriateness of branching versus linear time temporal logic for reasoning about concurrent programs are studied. These issues have been previously considered by Lamport. To facilitate a careful examination of these issues, a language, CTL*, in which a universal or existential path quantifier can prefix an arbitrary linear time assertion, is defined. The expressive power of a number of sublanguages is then compared. CTL* is also related to ...

7 Performance engineering case study: heap construction
Jesper Bojesen, Jyrki Katajainen, Maz Spork
December 2000 **Journal of Experimental Algorithmics (JEA)**, Volume 5

Full text available: pdf(474.71 KB) ps(537.43 KB) LaTeX(18.00 bytes)

Additional Information: full citation, abstract, references, citings, index terms

The behaviour of three methods for constructing a binary heap on a computer with a hierarchical memory is studied. The methods considered are the original one proposed by Williams [1964], in which elements are repeatedly inserted into a single heap; the improvement by Floyd [1964], in which small heaps are repeatedly merged to bigger heaps; and a recent method proposed, e.g., by Fadel et al. [1999] in which a heap is built layerwise. Both the worst-case number of instructions and that of cache m ...

Keywords: algorithms, binary heaps, code tuning, experimentation, memory tuning, performance, theory

8 Regular Articles: A blocked all-pairs shortest-paths algorithm
Gayathri Venkataraman, Sartaj Sahni, Srabani Mukhopadhyaya
January 2003 **Journal of Experimental Algorithmics (JEA)**, Volume 8

Full text available: pdf(282.82 KB) ps(318.10 KB)

Additional Information: full citation, abstract, references, index terms

We propose a blocked version of Floyd's all-pairs shortest-paths algorithm. The blocked algorithm makes better utilization of cache than does Floyd's original algorithm.

Experiments indicate that the blocked algorithm delivers a speedup (relative to the unblocked Floyd's algorithm) between 1.6 and 1.9 on a Sun Ultra Enterprise 4000/5000 for graphs that have between 480 and 3200 vertices. The measured speedup on an SGI O2 for graphs with between 240 and 1200 vertices is between 1.6 and 2.

Keywords: all pairs shortest paths, blocking, cache, speedup

9 "Sometimes" and "not never" revisited: on branching versus linear time (preliminary report)

E. Allen Emerson, Joseph Y. Halpern

January 1983 **Proceedings of the 10th ACM SIGACT-SIGPLAN symposium on Principles of programming languages**

Full text available: pdf(1.04 MB) Additional Information: full citation, abstract, references, citings

Temporal logic ([PR57], [PR67]) provides a formalism for describing the occurrence of events in time which is suitable for reasoning about concurrent programs (cf. [PN77]). In defining temporal logic, there are two possible views regarding the underlying nature of time. One is that time is linear: at each moment there is only one possible future. The other is that time has a branching, tree-like nature: at each moment, time may split into alternate courses representing different possi ...

10 Slicing floorplan with clustering constraints

Wing Seung Yuen, Fung Yu Young

January 2001 **Proceedings of the 2001 conference on Asia South Pacific design automation**

Full text available: pdf(360.33 KB) Additional Information: full citation, abstract, index terms

In floorplan design it is useful to allow users to specify placement constraints in the final packing. Clustering constraint is one kind of placement constraint in which a given set of modules are restricted to be geometrically adjacent to one another. The wiring cost can be reduced by putting modules with a lot of connections closely together. Designers may also need this type of placement constraint to pack the modules according to their functionality. In this paper, a method addressing c ...

11 The life cycle effects of software process improvement: a longitudinal analysis

Donald E. Harter, Mayuram S. Krishnan, Sandra A. Slaughter

December 1998 **Proceedings of the international conference on Information systems**

Full text available: pdf(32.71 KB) Additional Information: full citation, references, index terms

Keywords: IS development effort, IS development time, software quality

12 On the occur-check-free PROLOG programs

Krzysztof R. Apt, Alessandro Pellegrini

May 1994 **ACM Transactions on Programming Languages and Systems (TOPLAS)**, Volume 16 Issue 3

Full text available: pdf(2.43 MB) Additional Information: full citation, abstract, references, citings, index terms

In most PROLOG implementations, for efficiency occur-check is omitted from the unification algorithm. This paper provides natural syntactic conditions that allow the occur-check to be safely omitted. The established results apply to most well-known PROLOG programs, including those that use difference lists, and seem to explain why this omission does not lead in practice to any complications. When applying these results to general programs, we show their usefulness for proving absence of flo ...

Keywords: PROLOG programs, moded programs, occur-check problem, unification algorithm

13 PAC-learnability of Probabilistic Deterministic Finite State Automata
Alexander Clark, Franck Thollard
August 2004 **The Journal of Machine Learning Research**, Volume 5

Full text available: pdf(210.56 KB) Additional Information: full citation, abstract, index terms

We study the learnability of Probabilistic Deterministic Finite State Automata under a modified PAC-learning criterion. We argue that it is necessary to add additional parameters to the sample complexity polynomial, namely a bound on the expected length of strings generated from any state, and a bound on the distinguishability between states. With this, we demonstrate that the class of PDFAs is PAC-learnable using a variant of a standard state-merging algorithm and the Kullback-Leibler divergenc ...

Results 1 - 13 of 13

Terms used **ring integers authentication**

Found **76** of **151,219**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

☐ Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 76

Result page: **1** 2 3 4 next

Relevance scale

1 Protocols: A verifiable secret shuffle and its application to e-voting

C. Andrew Neff

November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security**

Full text available: pdf(216.76 KB) Additional Information: full citation, abstract, references, citings, index terms

We present a mathematical construct which provides a cryptographic protocol to *verifiably shuffle* a sequence of *k* modular integers, and discuss its application to secure, universally verifiable, multi-authority election schemes. The output of the shuffle operation is another sequence of *k* modular integers, each of which is the same secret power of a corresponding input element, but the order of elements in the output is kept secret. Though it is a trivial matter for the "shu ...

Keywords: anonymous credentials, electronic voting, honest-verifier, mix-net, permutation, universal verifiability, verifiable mix, verifiable shuffle, zeroknowledge

2 On randomization in sequential and distributed algorithms

Rajiv Gupta, Scott A. Smolka, Shaji Bhaskar

March 1994 **ACM Computing Surveys (CSUR)**, Volume 26 Issue 1

Full text available: pdf(8.01 MB) Additional Information: full citation, abstract, references, citings, index terms

Probabilistic, or randomized, algorithms are fast becoming as commonplace as conventional deterministic algorithms. This survey presents five techniques that have been widely used in the design of randomized algorithms. These techniques are illustrated using 12 randomized algorithms—both sequential and distributed— that span a wide range of applications, including:primality testing (a classical problem in number theory), interactive probabilistic proof s ...

Keywords: Byzantine agreement, CSP, analysis of algorithms, computational complexity, dining philosophers problem, distributed algorithms, graph isomorphism, hashing, interactive probabilistic proof systems, leader election, message routing, nearest-neighbors problem, perfect hashing, primality testing, probabilistic techniques, randomized or probabilistic algorithms, randomized quicksort, sequential algorithms, transitive tournaments, universal hashing

3 Chord: a scalable peer-to-peer lookup protocol for internet applications

Ion Stoica, Robert Morris, David Liben-Nowell, David R. Karger, M. Frans Kaashoek, Frank Dabek, Hari Balakrishnan

February 2003 **IEEE/ACM Transactions on Networking (TON)**, Volume 11 Issue 1

Full text available: pdf(690.54 KB) Additional Information: full citation, abstract, references, citings, index

terms

A fundamental problem that confronts peer-to-peer applications is the efficient location of the node that stores a desired data item. This paper presents *Chord*, a distributed lookup protocol that addresses this problem. Chord provides support for just one operation: given a key, it maps the key onto a node. Data location can be easily implemented on top of Chord by associating a key with each data item, and storing the key/data pair at the node to which the key maps. Chord adapts efficien ...

Keywords: distributed scalable algorithms, lookup protocols, peer-to-peer networks

4 Cryptographic sealing for information secrecy and authentication

David K. Gifford
April 1982 **Communications of the ACM**, Volume 25 Issue 4

Full text available: pdf(1.29 MB) Additional Information: full citation, abstract, references, citings, index terms

A new protection mechanism is described that provides general primitives for protection and authentication. The mechanism is based on the idea of sealing an object with a key. Sealed objects are self-authenticating, and in the absence of an appropriate set of keys, only provide information about the size of their contents. New keys can be freely created at any time, and keys can also be derived from existing keys with operators that include Key-And and Key-Or
Keywords: conentional crypto-systems, cryptographic sealing, key, seal, secrecy, unseal

5 Chord: A scalable peer-to-peer lookup service for internet applications

Ion Stoica, Robert Morris, David Karger, M. Frans Kaashoek, Hari Balakrishnan
August 2001 **ACM SIGCOMM Computer Communication Review , Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications**, Volume 31 Issue 4

Full text available: pdf(205.73 KB) Additional Information: full citation, references, citings, index terms

6 Group Key Management and Signatures: Provably authenticated group Diffie-Hellman key exchange

Emmanuel Bresson, Olivier Chevassut, David Pointcheval, Jean-Jacques Quisquater
November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security**

Full text available: pdf(578.14 KB) Additional Information: full citation, abstract, references, citings, index terms

Group Diffie-Hellman protocols for Authenticated Key Exchange (AKE) are designed to provide a pool of players with a shared secret key which may later be used, for example, to achieve multicast message integrity. Over the years, several schemes have been offered. However, no formal treatment for this cryptographic problem has ever been suggested. In this paper, we present a security model for this problem and use it to precisely define AKE (with "implicit" authentication) as the fundamental goal ...

7 Evaluation of an algorithm for finding a match of a distorted texture pattern in a large image database

N. Vujovic, D. Brzakovic
January 1998 **ACM Transactions on Information Systems (TOIS)**, Volume 16 Issue 1

Full text available: pdf(499.06 KB) Additional Information: full citation, abstract, references, index terms

Evaluation of an algorithm for finding a match for a random texture pattern in a large image database is presented. The algorithm was designed assuming that the random pattern may be subject to misregistration relative to its representation in the database and assuming that it may have missing parts. The potential applications involve authentication of legal documents, bank notes, or credit cards, where thin fibers are embedded randomly into the document medium during medium fabrication. Th ...

Keywords: image database, image matching, misregistration, presentation of information, random pattern

8 A comparison of ring and tree embedding for real-time group multicast

Mario Baldi, Yoram Ofek
June 2003 **IEEE/ACM Transactions on Networking (TON)**, Volume 11 Issue 3

Full text available: pdf(612.80 KB) Additional Information: full citation, abstract, references, index terms

In general topology networks, routing from one node to another over a tree embedded in the network is intuitively a good strategy, since it typically results in a route length of *O*(log *n*) links, being *n* the number of nodes in the network. Routing from one node to another over a ring embedded in the network would result in route length of *O(n)* links. However, in group (many-to-many) multicast, the overall number of links traversed by each packet, i.e., the networks ele ...

Keywords: communication systems, computer networks, flow control, multicast channels, multimedia communications, multimedia systems, real-time system, synchronization, timing

9 Combinatorial design of congestion-free networks

Bülent Yener, Yoram Ofek, Moti Yung
December 1997 **IEEE/ACM Transactions on Networking (TON)**, Volume 5 Issue 6

Full text available: pdf(317.84 KB) Additional Information: full citation, references, citings, index terms

10 The distributed firing squad problem

B A Coan, D Dolev, C Dwork, L Stockmeyer
December 1985 **Proceedings of the seventeenth annual ACM symposium on Theory of computing**

Full text available: pdf(1.09 MB) Additional Information: full citation, references, citings, index terms

11 An abstract interpretation-based framework for software watermarking

Patrick Cousot, Radhia Cousot
January 2004 **ACM SIGPLAN Notices , Proceedings of the 31st ACM SIGPLAN-SIGACT symposium on Principles of programming languages**, Volume 39 Issue 1

Full text available: pdf(171.12 KB) Additional Information: full citation, abstract, references, citings, index terms

Software watermarking consists in the intentional embedding of indelible stegosignatures or watermarks into the subject software and extraction of the stegosignatures embedded in the stegoprograms for purposes such as intellectual property protection. We introduce the novel concept of *abstract software watermarking*. The basic idea is that the watermark is hidden in the program code in such a way that it can only be extracted by an abstract interpretation of the (maybe non-standard) concre ...

Keywords: abstract interpretation, authentication, copyrights protection, fingerprinting, identification, intellectual property protection, obfuscation, software authorship, software watermarking, static analysis, steganography, stegoanalyst, stegoattacks, stegokey, stegomark, stegosignature, tamper-proofing, trustworthiness, validation watermarking

12 Low power scalable encryption for wireless systems

James Goodman, Anantha P. Chandrakasan
January 1998 **Wireless Networks**, Volume 4 Issue 1

Full text available: pdf(7.39 MB) Additional Information: full citation, abstract, references, index terms

Secure transmission of multimedia information (e.g., voice, video, data, etc.) is critical in

many wireless network applications. Wireless transmission imposes constraints not found in typical wired systems such as low power consumption, tolerance to high bit error rates, and scalability. A variety of low power techniques have been developed to reduce the power of several encryption algorithms. One key idea involves exploiting the variation in computation requirements to dynamically vary th ...

13 Distributed operating systems

Andrew S. Tanenbaum, Robbert Van Renesse
December 1985 **ACM Computing Surveys (CSUR)**, Volume 17 Issue 4

Full text available: pdf(5.49 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Distributed operating systems have many aspects in common with centralized ones, but they also differ in certain ways. This paper is intended as an introduction to distributed operating systems, and especially to current university research about them. After a discussion of what constitutes a distributed operating system and how it is distinguished from a computer network, various key design issues are discussed. Then several examples of current research projects are examined in some detail ...

14 Secure password-based cipher suite for TLS

May 2001 **ACM Transactions on Information and System Security (TISSEC)**, Volume 4 Issue 2

Full text available: pdf(507.57 KB) Additional Information: full citation, abstract, references, citings, index terms, review

SSL is the de facto standard today for securing end-to-end transport on the Internet. While the protocol itself seems rather secure, there are a number of risks that lurk in its use, for example, in web banking. However, the adoption of password-based key-exchange protocols can overcome some of these problems. We propose the integration of such a protocol (DH-EKE) in the TLS protocol, the standardization of SSL by IETF. The resulting protocol provides secure mutual authentication and key establi ...

Keywords: Authenticated key exchange, dictionary attack, key agreement, password, perfect forward secrecy, secure channel, transport layer security, weak secret

15 Non-interactive and non-malleable commitment

Giovanni Di Crescenzo, Yuval Ishai, Rafail Ostrovsky
May 1998 **Proceedings of the thirtieth annual ACM symposium on Theory of computing**

Full text available: pdf(1.50 MB) Additional Information: full citation, references, citings, index terms

16 Network Protocols

Andrew S. Tanenbaum
December 1981 **ACM Computing Surveys (CSUR)**, Volume 13 Issue 4

Full text available: pdf(3.37 MB) Additional Information: full citation, references, citings, index terms

17 Fast and flexible application-level networking on exokernel systems

Gregory R. Ganger, Dawson R. Engler, M. Frans Kaashoek, Héctor M. Briceño, Russell Hunt, Thomas Pinckney
February 2002 **ACM Transactions on Computer Systems (TOCS)**, Volume 20 Issue 1

Full text available: pdf(500.67 KB) Additional Information: full citation, abstract, references, citings, index terms

Application-level networking is a promising software organization for improving performance and functionality for important network services. The Xok/ExOS exokernel system includes application-level support for standard network services, while at the same time allowing application writers to specialize networking services. This paper describes how Xok/ExOS's kernel mechanisms and library operating system organization achieve this

flexibility, and retrospectively shares our experiences an ...

Keywords: Extensible systems, OS structure, fast servers, network services

18 Trustworthy 100-year digital objects: Evidence after every witness is dead

Henry M. Gladney

July 2004 **ACM Transactions on Information Systems (TOIS)**, Volume 22 Issue 3

Full text available: pdf(1.24 MB) Additional Information: full citation, abstract, references, index terms

In ancient times, wax seals impressed with signet rings were affixed to documents as evidence of their authenticity. A digital counterpart is a message authentication code fixed firmly to each important document. If a digital object is sealed together with its own audit trail, each user can examine this evidence to decide whether to trust the content---no matter how distant this user is in time, space, and social affiliation from the document's source.We propose an architecture and design that a ...

19 Key establishment in sensor networks: Connectivity properties of secure wireless sensor networks

Roberto Di Pietro, Luigi V. Mancini, Alessandro Mei, Alessandro Panconesi, Jaikumar Radhakrishnan

October 2004 **Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks**

Full text available: pdf(257.22 KB) Additional Information: full citation, abstract, references, index terms

We address the problem of connectivity in Secure Wireless Sensor Networks (SWSN) using random pre-distribution of keys. We propose a geometric random model for SWSNs. Under this new and realistic model, we describe how to design secure and connected networks using a small constant number of keys per sensor. Extensive simulations support the above stated result and demonstrate how connectivity can be guaranteed for a wide interval of practical network sizes and sensor communication ranges.

Keywords: connectivity, key management, probabilistic key sharing, random graphs, sensor networks

20 Getting started with PGP

Kevin Henry

July 2000 **Crossroads**, Volume 6 Issue 5

Full text available: html(37.59 KB) Additional Information: full citation, index terms

WEB RESULTS by Google (Showing Results 1 - 10 of 133)

1. Practical Identification Schemes as Secure as the DL and RSA ...
... iden- tification scheme, ID-RSA, which is proven to be as secure as the RSA problem and alm efficient as the **Guillou-Quisquater** identification scheme ...
grouper.ieee.org/groups/1363/StudyGroup/contributions/id-dl.pdf

2. Practical Identification Schemes as Secure as the DL and RSA ...
... identification scheme, ID-RSA, which is proven to be as secure as the RSA problem and almo as the **Guillou-Quisquater** identification scheme; the ...
grouper.ieee.org/groups/1363/StudyGroup/contributions/id-dl.ps

3. 1 Introduction
... ElGamal public key cryptosystem and S = **Guillou- Quisquater** signature scheme 10 , as wil in Section 6. 4 Description and Analysis of New Protocols ...
doi.ieeecomputersociety.org/10.1109/SECPRI.1998.674825

4. Errata of IACR Publications
... The protocol can also be seen as a generalization of the identification protocol by **Guillou-Qu** [GQ]. Where [GQ] is L.**Guillou** ...
www.iacr.org/newsletter/v15n1/errata.html - 2 KB

5. Anonymous Authentication With Subset Queries
... For example, the scheme can be built on top of **Guillou-Quisquater** authentication [20]. ... 4 [20] L. **Guillou** and JJ **Quisquater**, "A practical zero- ...
crypto.stanford.edu/~dabo/papers/annonauth.ps - 0 B

6. Concurrent Zero-Knowledge is Easy in Practice
... The construction behind this result can be applied in practice to the well known proofs of kno Schnorr and **Guillou-Quisquater** to yield concurrent zero ...
philby.ucsd.edu/cryptolib/psfiles/99-14.ps - 0 B

7. Modern Encryption Methods in User Authentication
... Some examples on zero-knowledge protocols are Fiat-Shamir, Feige-Fiat-Shamir (FFS), and **G Quisquater** (GQ). 2. Strong Authentication ...
www.hut.fi/~lhuovine/study/netsec97/user_auth.html - 57 KB

8. Table of Contents
... Scheme; The Okamoto Identification Scheme; The **Guillou-Quisquater** Identification Schem based Identification Schemes. Converting ...
www.cacr.math.uwaterloo.ca/~dstinson/contents.html - 7 KB

9. Keyword Index
... group signatures c87-120 e89-56 e91-257 c91-457 e94-171 e94-194 e95-39 e97-465 c97-4 **Quisquater** identification scheme (see identification) hard core ...
dsns.csie.nctu.edu.tw/research/crypto/HTML/KEYWORDS.HTM - 101 KB

10. Q107: What are Interactive Proofs and Zero-Knowledge Proofs?
... **Guillou** and **Quisquater** [GQ88] further improved Fiat-Shamir's protocol in terms of memory requirements and interaction (the number of rounds in the protocol). ...
www.x5.net/faqs/crypto/q107.html - 6 KB

Search for "**guillou quisquater**" using: Ask Jeeves

WEB RESULTS by Google (Showing Results 1 - 10 of 150)

1. **gQ2**
The Interface. gQ's interface consists of several components. The twelve bands in the center of provide the primary controls. ...
www.music.princeton.edu/~dan/gQpage/gQ2.html - 6 KB

2. Bienvenue sur la page d'accueil du FLG
Vous souvenez vous de Groquik . disparu des boites de Nesquik il ya 6 ans. Remplacé par un af nous n'avions plus de nouvelles. ...
www.groquik.8m.com/gq2.htm - 9 KB

3. **GQ2**????????
The summary for this Japanese page contains characters that cannot be correctly displayed in t language/character set.
www2u.biglobe.ne.jp/~caveofts/bbs/940338134765625.html - 2 KB

4. **GQ2**????????...
The summary for this Japanese page contains characters that cannot be correctly displayed in t language/character set.
www2u.biglobe.ne.jp/~caveofts/bbs/64654541015625.html - 2 KB

5. Lattice file of KEK PS Main Ring. (SAD format) ! ! Original file ...
... QDE = (L= 0.61505 K1=-0.1342905) GQ1= (L= 0.225 K1=+0.01504) **GQ2**= (L= 0.225 K 0.01504) ; BEND B = (L= 3.2575 ANGLE= 7.5 DEG E1= 0.250 E2= 0.250 ...
www-accps.kek.jp/info/database/OLD/lattice.MR - 5 KB

6. VTEDIT.TEC V02.02![00 0X010U0[0ETU0[0 0 32ET U032 0ETQ0"LOSKPCHK ...
... Q7-127"E.-Q5"L.U5'.-Q5+1U2ODEL '!.C!!LC!!PC!!QC!!SC!0Q3"NQ7I F<'MM0U20U40U60U31 64M3-10"NOERR '0U3 2 !CRL!Q5<13I 10I > Q5*Q3R!LMG!Q0U2Q2"**GQ2**/8U2Q2<9I ...
www.ibiblio.org/pub/academic/computer-science/history/pdp-11/rt/sigtapes/fa - 12 KB

7. "Bookshelf" Effect Tolerance
... E VITM = - 2Q2/Jlm(I-(-1)qe-ikz) 2b(**Gq2** - k212) TMlmq mode, magnetic field kick, H 6TM = (-I)qemikz) 2b(**Gq2** - k212) TE1mq mode, electric field kick, ...
www-project.slac.stanford.edu/lc/local/AccelPhysics/Main%20Linac/Meetings/g - 0 B

8. GUNSLINGER QUAKE (1.0) ---------- Welcome to ...
... Any standard Quake2 multiplayer map can be used with Gunslinger Quake (items are replace items). ... **GQ2** has a special command for it. ...
www.rps.net/gunslinger/readme.html - 28 KB

9. VTEDIT.TEC V39.00![00 0X010U0[0EDU0[0ETU0[0 0ED0 32ET U032 0ETQ0"L ....
... Q5<13I 10I >Q5*Q3R!LMG!9Q0- I"EM2F<'!TAB!Q0U2Q2"**GQ2**/8U2Q2& lt;9I > Q2* Q2<32I > M2F<![C!64M3-32"LQ7Q0U9O^EU9CE 'Q7- O"EETU80 4ET 64M3 Q8&4"E4 0ET'Q7"AQ7&32 ...
sunsite.tus.ac.jp/pub/academic/computer-science/history/pdp-11/teco/rsts/vt - 13 KB

10. VTEDIT.TEC V39.00![00 0X010U0[0EDU0[0ETU0[0 0ED0 32ET U032 0ETQ0" ...
... F<!AC!@ 2/< "T.U9ZJ12I Q9J'/OAPN !BC!.U9Q5<-.;RS^N^EG1 ;RS^EG1 ;>.+1U2Q Q5+1"EHKEK 4Output killed, e OXIT ' 0 OXM0 !CC!0;!DC!Q5 U2Q2"**GQ2**-1A-10"E-1%2 ...

WEB RESULTS by Google (Showing Results 1 - 10 of 223)

1. Table of Contents List of Tables xv List of Figures xix Foreword ...
... of **authentication** in ... Blum **integers** : : : : : ... 2 Rings : : : : : ...
www.cacr.math.uwaterloo.ca/hac/about/toc3.ps - 0 B

2. Discrete logarithms in finite fields and their cryptographic ...
... to compute appears to be an **authentication** scheme. ... **integers** chosen by the two users. the matrix **ring** generated by B is isomorphic to the field ...
www.dtc.umn.edu/~odlyzko/doc/arch/discrete.logs.pdf - 0 B

3. PH "" .EQ delim $$ define Run % bold R % define vun % bold v % .EN .....
... to compute appears to be an **authentication** scheme. ... a$ and b are the two random **int** chosen by ... However, the matrix **ring** generated by B is isomorphic to ...
www.dtc.umn.edu/~odlyzko/doc/arch/discrete.logs.troff - 101 KB

4. UMAC: Fast and Secure Message **Authentication**
... hashing paradigm has reduced the problem of fast message **authentication** to that ... and de being defined using two different rings, Z/2 ... signed **integers**). ...
www.cs.ucdavis.edu/~rogaway/umac/umac_proc.pdf - 0 B

5. UMAC: Fast and Secure Message **Authentication**
... Computing the **authentication** tag: ... **integers** and back, leaving this to the reader's good s <= n. Since ad-dition and multiplication in a **ring** are commutative ...
www.cs.ucdavis.edu/~rogaway/umac/umac_proc.ps - 0 B

6. Course Listing For MATH
... fractions, sums of two squares and Gaussian **integers**. ... key exchange systems, signature **authentication**, public key ... the spectrum of a **ring**, "gluing" spectra to ...
bulletin.uga.edu/summer1999/bulletin/courses/descript/math.html - 54 KB

7. Digital Signature Schemes
... Theory 213 8.1.2 Basic Facts about Rings of **Integers** ... Blum **Integers** 216 8.1.4 Williams **I** 217 8.1 ... Hashing 313 10.2 Bottom-up Tree **Authentication** 322 10.3 ...
www.semper.org/sirene/people/birgit/BlurbPfit8_96.html - 16 KB

8. Za-Zm
... **ring** (including Karatsuba multiplication for large **integers**); ... on elliptic curves over any fin protocol, with the **authentication** usually provided by ...
stommel.tamu.edu/~baum/linuxlist/tempo/node56.html - 21 KB

9. Protection and Security
... if current **ring** is above bracket but within "limit ... A trusted authority can also facilitate **auth** (signatures ... represent it as a string of **integers** in the ...
www.cs.rochester.edu/u/www/courses/456/spring99/lecture/lecture13.html - 26 KB

10. A Method for Obtaining Digital Signatures and Public-Key ...
... In an **authentication** problem the recipient does not worry about this possibility ... to OE(n), multiplicative inverse e in the **ring** of **integers** modulo OE ...
theory.lcs.mit.edu/~cis/pubs/rivest/rsapaper.ps - 0 B

Search for "**ring integers authentication**" using: Ask Jeeves